



# PHILIPS

## Security Testing Report

EDI\Interoperability Solutions

XDS 2023-2

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Table of Contents

Document Version Control.....	3
Document History .....	3
Distribution List .....	5
1. Definitions & Abbreviations .....	6
2. System Details & Architecture.....	7
3. Scope .....	9
4. Out of Scope.....	10
5. Executive Summary .....	11
6. Vulnerability Summary .....	13
7. Observations.....	15
8. Detailed Vulnerability Report.....	17
8.1 Webapp: Using Known Vulnerable Components .....	17
8.2 Webapp: Broken Access Control .....	23
8.3 Webapp: Weak Password Policy .....	30
8.4 Webapp: DOM Cross-Site Scripting (XSS).....	34
8.5 Webapp: Weak Input Validation .....	39
8.6 Webapp: Improper Error & Exception Handling .....	43
8.7 Webapp: Sensitive Information in the URL .....	47
8.8 Webapp: HTTP Strict Transport Security (HSTS) Not Implemented.....	50
8.9 Webapp: No Account Lockout Policy .....	53
8.10 Webapp: Reflected Cross-Site Scripting (XSS).....	57
8.11 Webapp: Weak SSL/TLS Configuration.....	63
8.12 Webapp: Missing Security Header .....	68
8.13 Webapp: Server Banner Disclosure.....	70
9. Tools Used .....	72
10. Automated Tool Report.....	72
11. Manual Test Reports and Test Case Execution .....	72

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Document Version Control

Name of the document : XDS 2023-2 Security Testing Report		
Version: 8.0	Intake ID:	2764
<b>Document Definition:</b> This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate vulnerabilities.	Document ID:	PRHC/C40/SVN/87857
<b>Author:</b> Sai Praneetha Bhaskaruni, Harshal Kukade	Effective Date:	25/Oct/2023
<b>Reviewed by:</b> Chaitra N Shivayogimath		

## Document History

Version	Date	Author	Section	Changes
0.1	20/Jul/2020	Narendra Makkena	Complete	Initial Draft
1.0	20/Jul/2020	Taksh Medhavi	Complete	Addition & review
1.1	01/Mar/2021	Shabana Bagum	Complete	Initial Draft
1.2	02/Mar/2021	K K Ashwin	Complete	Addition & review
2.0	03/Mar/2021	Narendra Makkena	Complete	Final review
2.1	03/March/2022	Shibija K	Complete	Initial Draft
2.2	04/March/2022	K K Ashwin	Complete	Addition & review
3.0	04/March/2022	Pranati Mohanty	Complete	Final review

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



3.1	27/May/2022	Sreerag M	Vuln 8.2,8.4,8.6 and 8.11	Retest
3.2	27/May/2022	Shibija K	Vuln 8.2,8.4,8.6 and 8.11	Addition & review
4.0	27/May/2022	Pranati Mohanty	Vuln 8.2,8.4,8.6 and 8.11	Final Review
4.1	27/Aug/2022	Kartik Lalan	Complete	Addition & review
5.0	29/Aug/2022	Shibija K	Complete	Final Review
5.1	31/Jan/2023	Ashwin K K	Vuln 8.2,8.4,8.6 and 8.11	New feaure and retest
5.2	01/Feb/2023	Shibija K	Complete	Addition & technical review
6.0	01/ Feb /2023	Pranati Mohanty	Complete	Final Review
6.1	08/Jun/2023	Raj Kiran Rudrapati	Complete	Issue revalidation & Rapid test
7.0	09/Jun/2023	Aravind C Ajayan	Complete	Addition & Review
7.1	25/Oct/2023	Sai Praneetha Bhaskaruni, Harshal Kukade	Complete	Addition & Retest
8.0	25/Oct/2023	Chaitra N Shivayogimath	Complete	Final Review

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	<a href="mailto:subhash.naga@philips.com">subhash.naga@philips.com</a> ; <a href="mailto:Stephanie.Heidstra@philips.com">Stephanie.Heidstra@philips.com</a> ; <a href="mailto:moin.creemers@philips.com">moin.creemers@philips.com</a> ; <a href="mailto:ManishKumar.MachingalSukumar@philips.com">ManishKumar.MachingalSukumar@philips.com</a> ; <a href="mailto:Stephanie.Heidstra@philips.com">Stephanie.Heidstra@philips.com</a> ; <a href="mailto:chidamber.kumar_1@philips.com">chidamber.kumar_1@philips.com</a> ; <a href="mailto:abhishek.kumar.pathak@philips.com">abhishek.kumar.pathak@philips.com</a> ; <a href="mailto:revathi.r@philips.com">revathi.r@philips.com</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below:

None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located [here](#). Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016
IoT/Hardware security assessment	OWASP Top Ten – 2014

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 2. System Details & Architecture

Brief about the product architecture:

Philips Interoperability Solutions (formerly Forcare) is an open-standard-based interoperability software solutions for fast and flawless data flows between medical systems and information sources at the departmental and enterprise levels, as well as Health Information Exchanges (HIEs) across health systems.

The tested components: ForView, ForAudit ForImageUpload and ForAdmin web application.

**ForAdmin** - ForAdmin is a web-based application for system administrators. This can be used for configuring and monitoring the Forcare application components in your network. With ForAdmin, you can make configuration changes at runtime without requiring restarting your server. Component configurations are stored in XML files that are validated to prevent basic configuration errors.

**ForView**- ForView is an application for care providers that lets them find, view, and share patient-oriented clinical information. ForView complements existing clinical information systems, adding the ability to view documents and images from a variety of sources that are not limited to one specific institution or document type.

**ForAudit**- ForAudit is an IHE ATNA Audit Repository. It captures audit logs sent via UDP or TCP/SSL (syslog, per IHE ITI ATNA) and supports HTTP or HTTPS based audit transactions.

**ForImageUpload**- ForImageUpload is an application to upload Dicom/Zip files of images.

PHILIPS SCOE

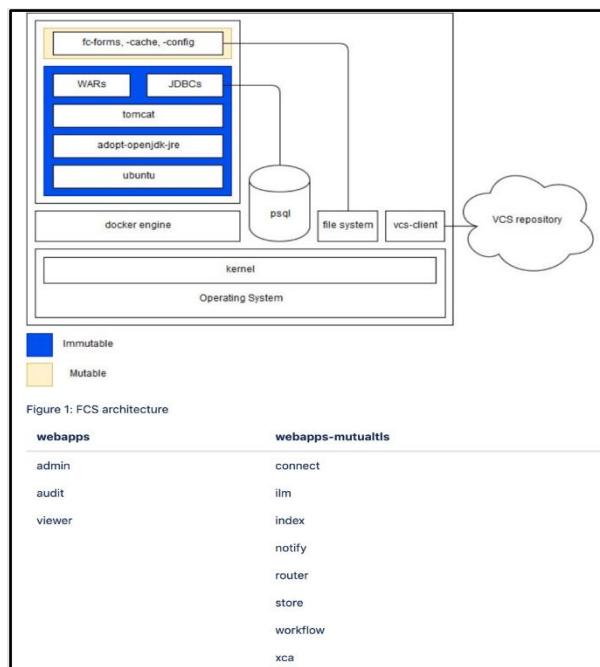


Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The environment provided for security testing is a Pentest Environment.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



### 3. Scope

The scope of this security assessment is to perform **Grey box** security testing to find security threats that may come from a malicious outsider or insider user of the **XDS 2023-2**. Security testing on **Web applications (Viewer, Audit, Admin, & ImageUpload)** of **XDS 2023-2** is performed.

The following list includes some examples of major activities performed during the assessment:

#### Web Application:

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection-based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.

*Follow “[Test case execution](#)” section to get the detailed about test*

Type	Scope of Assessment		
Web Application	XDS 2023-2	URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload/">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload/</a>
		Version	2023-2
		Environment	Pentest
		User Roles	root (Self Creatable User Roles)



## 4. Out of Scope

Below mentioned items are out of scope for the current security assessment:

- Source code review
- Cloud Testing
- Docker Testing
- Complete security assessment of 4 portals

**Note:** We have covered the testing of **XDS 2023-2** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 5. Executive Summary

Security Center of Excellence (SCoE) team is engaged in activities to conduct security assessment of **XDS 2023-2** which included **Web applications** in scope. The purpose of the engagement is to evaluate the security of the **XDS 2023-2** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment following factors are found with consideration for significant improvement:

- Using known vulnerable components
- Broken Access Control
- Security Misconfigurations

During the security assessment of the product, security issues in the below areas are not found:

- Injection attacks

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

**Note:** The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.

Critical	High	Medium	Low
0	0	3	8

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 6. Vulnerability Summary

The findings and vulnerabilities from the assessment are explained in the below table:

Finding No.	Vulnerability Title	Technical Risk	Impacted Area	CVE ID*	Status	Status (23-Oct-23)
30132	Using Known vulnerable components	Medium	Webapp	Refer 8.1	Open	Open
79143	Broken Access Control	Medium	Webapp	NA	Open	Open
30136	Weak Password Policy	Medium	Webapp	NA	Open	Open
77505	DOM Cross Site Scripting	Low	Webapp	NA	Open	CLOSED
30145	Weak Input Validation	Low	Webapp	NA	Open	Open
30209	Improper error & exception handling	Low	Webapp	NA	Open	Open
37688	Sensitive information in the URL	Low	Webapp	NA	Open	Open
30128	HTTP Strict Transport Security (HSTS) Not Implemented	Low	Webapp	NA	Open	Open
30146	No Account Lockout Policy	Low	Webapp	NA	Open	Open
30125	Reflected Cross-Site Scripting (XSS)	Low	Webapp	NA	Open	CLOSED

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



83850	Weak SSL/TLS Configuration	Low	Webapp	NA	Open	Open
88944	Missing Security Header	Low	Webapp	NA	-	Open
88946	Server Banner Disclosure	Low	Webapp	NA	-	Open

\*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 7. Observations

Below mentioned observations are not considered as vulnerability but informative to the business.

*Observations which shows good implementation or best practice identified:*

- XSS protection flag is enabled.

Request		Response			
Pretty	Raw	Hex	Pretty	Raw	Render
1 GET /viewer/services/domain/list.json HTTP/2			1 HTTP/2 200 OK		
2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com			2 Cache-Control: no-store, no-cache, must-revalidate		
3 Cookie: JSESSIONID=50BCA220735453D809EB54F3CAC7DC27			3 Cache-Control: post-check=0, pre-check=0		
4 Sec-Ch-Ua:			4 Content-Type: application/json; charset=UTF-8		
5 Content-Type: application/x-www-form-urlencoded			5 Date: Sat, 21 Oct 2023 10:38:36 GMT		
6 X-Requested-With: XMLHttpRequest			6 Expires: 0		
7 Sec-Ch-Ua-Mobile: ?0			7 Forcare.com-Logcontext: 79a8f001e495/viewer-24272		
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)			8 X-Content-Type-Options: nosniff		
Chrome/115.0.5790.110 Safari/537.36			9 X-Frame-Options: SAMEORIGIN		
9 Sec-Ch-Ua-Platform: "			10 X-Xss-Protection: 1; mode=block		
10 Accept: */*			11 Content-Length: 329		
11 Sec-Fetch-Site: same-origin			12		
12 Sec-Fetch-Mode: cors			13 {		
13 Sec-Fetch-Dest: empty			"identifier": "id",		
14 Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html			"allowPatientIdQueryWithoutDomain": false,		
15 Accept-Encoding: gzip, deflate			"targetDomain": "",		
16 Accept-Language: en-US,en;q=0.9			"items": [		
17			{		
18			"id": "1.3.6.1.4.1.21367.2005.3.8",		
			"name": "Hospital",		
			"shortName": "HOS"		
			},		
			{		
			"id": "1.3.6.1.4.1.21367.2005.3.7",		
			"name": "Intellispace Exchange",		
			"shortName": "ISX"		
			},		
			{		
			"id": "2.16.040.1.113083.2.1.4.1",		
			"name": "Citizen Service Number",		
			"shortName": "BSN"		
			}		
			}		

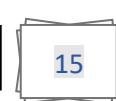
- The usage of the required HTTP methods has been defined properly at the server end. Which means if a GET request is used and if a different request is tried, then the server responds with "405" method not allowed error which is a good observation.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



*Observations which shows missing best practice or possible weak implementation (this may/may not be direct active threat):*

- No email verification while registering the user.
- Application allows simultaneous session logons.
- Password is in plain text at admin portal in the configurations.

- ImageUpload Online help page does not require any authentication. Since there is no PII or PHI we are marking this as Observation.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8. Detailed Vulnerability Report

### 8.1 Webapp: Using Known Vulnerable Components

Vulnerability Title	Using Known Vulnerable Components
Vulnerability Category	A6 Vulnerable and Outdated Components
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.8 CVSS:3.0/ AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the product, it is observed that the web application is using components with known vulnerabilities and associated CVEs.</p> <p>Technologies are like jquery-1.2.6, dojo 1.9.6 and AngularJS v1.8.2 have known CVE IDs:</p> <p>jquery-1.2.6, AngularJS v1.8.2, and dojo 1.9.6</p> <ul style="list-style-type: none"> <li>• moment.js 2.29.3 - <a href="#">CVE-2022-31129</a></li> <li>• jquery-1.2.6 - <a href="https://nvd.nist.gov/vuln/detail/CVE-2011-4969">https://nvd.nist.gov/vuln/detail/CVE-2011-4969</a></li> <li>• AngularJS v1.8.2 - <a href="#">angular 1.8.2 vulnerabilities   Snyk</a></li> <li>• Dojo 1.9.6 - <a href="https://security.snyk.io/package/npm/dojo/1.9.2">https://security.snyk.io/package/npm/dojo/1.9.2</a></li> </ul> <p>AngularJS LTS discontinued.</p> <p><a href="#">Discontinued Long Term Support for AngularJS   by Mark Thompson (@marktechson)   Angular Blog</a></p> <p><b>Retest (23-October-2023):</b> All the mentioned vulnerable components are still present in this application.</p> <p><b>Exploitability Rational:</b> Published vulnerabilities have a greater likelihood of exploitation by attackers due to readily available proof-of-concept code that exploits the issue or integrates the exploits into freely available testing tools.</p> <p><b>Impact Rational:</b> Depending on the nature of known vulnerabilities, this can allow an attacker to compromise the server and any data stored within.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a>
Recommendation	Service version is vulnerable to an attack, take preventative measures to mitigate the vulnerability until an upgrade or patch is released.
Status	<b>OPEN</b>

#### Steps to Reproduce:

**Retested (23<sup>rd</sup> October 2023):**

Steps to Reproduce:

- Launch the application and run retire.js plugin.
- Login to any application ForAdmin, ForView, ForAudit.

#### Supported Evidences:

For View Portal:

The screenshot shows the Retire.js extension interface in a browser window. The URL is https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient. The extension is enabled. The interface lists three dependencies with their versions and associated vulnerabilities:

- angularjs** 1.8.2: Found in https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/2302-12/js/angular/angular.min.js - Vulnerability info: Low End-of-Life: Long term support for AngularJS has been discontinued 54 [1]
- dojo** 1.9.6: Found in https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/2302-12/js/dojo/dojo.js - Vulnerability info: High CVE-2018-15494 [1], High CVE-2020-5258 GHSA-jxth-8wgv-vfr2 [1], High Prototype pollution CVE-2021-23450 GHSA-m8gw-hjpr-rjv7 [1]
- jquery** 1.2.6: Found in https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/2302-12/js/simile-ajax/simile-ajax-bundle.js - Vulnerability info: Medium CVE-2011-4969 XSS with location.hash GHSA-579v-mp3v-rn5 [1] [2] [3], Medium CVE-2012-6708 11290 Selector interpreted as HTML GHSA-2pj-3hvj-pggw [1] [2] [3], Medium CVE-2020-7656 Versions of jquery prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e. "</script >", which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser. [1] [2]

At the bottom, there is a note: ## Recommendation.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient

logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

## Recommendation

Upgrade to version 1.9.0 or later. GHSA-q4m3-2j7h-f7xw [1] [2] [3]

Medium CVE-2019-11358 4333 jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery extend(true, {}, ...) because of Object prototype pollution GHSA-6c3jc64m-qhgq [1]

Medium CVE-2020-11022 4642 Regex in its jQuery.htmlPrefilter sometimes may introduce XSS GHSA-gxr4-xjj5-5px2 [1]

Medium CVE-2020-11023 CVE-2020-23064 4647 passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. GHSA-jpcq-cgw6-v4j6 [1]

Low 73 jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates [1]

moment.js 2.29.3 Found in https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/2302-12/js/moment/moment.min.js - Vulnerability info: High Regular Expression Denial of Service (ReDoS). Affecting moment package, versions >=2.18.0 <2.29.4 CVE-2022-31129 GHSA-wc69-hjpr-hc9g [1] [2]

**Save**

#### For Admin Portal:

https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/login.html#

**Retire.js**  Enabled  Show unknown

dojo	1.9.6	Found in https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/2302-22js/dojo/dojo.js - Vulnerability info:
		High CVE-2018-15494 [1]
		High CVE-2020-5258 GHSA-jxth-8wgv-vfr2 [1]
		High Prototype pollution CVE-2021-23450 GHSA-m8gw-hjpr-rjv7 [1]

**Save**

#### For Audit Portal:

https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit/index.html

es. Set filter criteria to narrow the result.

Patient ID	User	Audit Source
	uid=root,dc=domain,dc=local	a8ac29a8a030
	uid=root,dc=domain,dc=local	f90178012241/

**Retire.js**  Enabled  Show unknown

dojo	1.9.6	Found in https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit/2302-15js/dojo/dojo.js - Vulnerability info:
		High CVE-2018-15494 [1]
		High CVE-2020-5258 GHSA-jxth-8wgv-vfr2 [1]
		High Prototype pollution CVE-2021-23450 GHSA-m8gw-hjpr-rjv7 [1]

**Save**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Steps same as before

The screenshot shows a browser window with a Retire.js plugin vulnerability report for the dojo 1.9.6 library. The report details several security issues, including Medium severity CVE-2018-15494 and High severity CVE-2020-5258. Below the report is a login page for 'FORADMIN'.

audit\_login\_pg\_onl  
y.html

viewer\_retirejs.html

The screenshot shows a browser window displaying an HTTP Status 404 – Not Found error page from Apache Tomcat/9.0.71. The message indicates that the requested resource [/viewer/patient/] is not available.

Old POC:

- Launch the application and run retire.js plugin.
- Login to any application ForAdmin, ForView.

ForView Portal

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Not secure | <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/patient/query.html>

Enabled

### Retire.js

angularjs	1.8.2	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/angular/angular.min.js Vulnerability info: Low End-of-Life: Long term support for AngularJS has been discontinued 54	[1]
angularjs	1.8.2	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/angular/angular.min.js Vulnerability info: Low End-of-Life: Long term support for AngularJS has been discontinued 54	[1]
dojo	1.9.6	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/dojo/dojo.js Vulnerability info: Medium 307 [1] [2] High CVE-2018-15494 [1] Medium CVE-2020-5258 [1] Medium Prototype pollution CVE-2021-23450 [1]	
jquery	1.2.6	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/simile-ajax/simile-ajax-bundle.js Vulnerability info: Medium CVE-2011-4969 XSS with location.hash [1] [2] Medium CVE-2012-6708 11290 Selector interpreted as HTML [1] [2] [3] Medium CVE-2019-11358 jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution [1] [2] Medium CVE-2020-11022 Regex in its jQuery.htmlPrefilter sometimes may [1]	

## ForAdmin portal

Not secure | <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/admin/overview.html>

Enabled

### Retire.js

dojo	1.9.6	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/2204-46/js/dojo/dojo.js Vulnerability info: Medium 307 [1] [2] High CVE-2018-15494 [1] Medium CVE-2020-5258 [1] Medium Prototype pollution CVE-2021-23450 [1]	
------	-------	---	--

Banner grabbing of Apache Tomcat server version.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



← → ⌂ https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/patient/

## HTTP Status 404 – Not Found

**Type** Status Report

**Message** The requested resource [/viewer/patient/] is not available

**Description** The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

**Apache Tomcat/9.0.68**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.2 Webapp: Broken Access Control

Vulnerability Title	Broken Access Control
Vulnerability Category	A1 Broken Access Control
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 6.5 CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>The application allows lower privileged users to access resources or perform actions which is available to a higher-level account. This usually occurs when the server does not perform authorization/entitlement checks on each request to ensure that the user has the appropriate privileges before executing the request, or when those checks are made based on values that can be tampered with on the client-side.</p> <p>It is observed that the user without SYSTEM_PHI_READ role defined can view/read the following API endpoints which consists of sensitive information like, backend components/versions, encryption password etc.</p> <p><b>Retest (23-Oct-2023):</b></p> <p>It is observed that user with SYSTEM_PHI_READ has view option on backend configuration which includes sensitive information. Issue still persists.</p> <p><b>Exploitability Rational:</b></p> <p>The attacker can be any user who has access to the forcare admin application.</p> <p><b>Impact Rational:</b></p> <p>Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which can allow user impersonation (in the event of credential or session identifier).</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/services/admin/components/viewer/config/properties.json">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/services/admin/components/viewer/config/properties.json</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<b>Note:</b> This is an application wide issue. Instances are not limited to the above items. Fix should be applied across the platform.
<b>Recommendation</b>	Check and verify the privileges of the user and check or verify before serving the response.
<b>Status</b>	<b>OPEN</b>

### Steps to Reproduce:

#### Retest (23-Oct-2023):

##### Case 1:

Step1: Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Leave the setup idle for about 5-10mins, the token becomes unauthorized.

Step3: Send the retrieve data request to repeater and observe the behavior.

#### Supported Evidences:

```

Target: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
HTTP/2

Request
Pretty Raw Hex
1 GET /admin/services/admin/components/viewer/config/properties.json HTTP/2.0
2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
3 Cookie: JSESSIONID=B4AB261439748301080317ABD1F3B9
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Authorization: Bearer eyJhbGciOiJSUzIiNtisInglidCIjEiJFLkmoQt8ER4eEgtZkZjeX1Xby1DTmpnvvFCyJ9.eyJpcjMioiJcm46b2lk0jzuM140iLwLYXVXKijoiHR0cHm6Ly9sbNhbGhvC3q60DA4NS92aw3ZxIiL
CjzdwIi0jyb290i1wiu3ViAmyd8IEtjoiLcm9vdCis1KnkbhmuaWhhbFvZxJJZC16invp2DiY
b29ULGRjFWWbWPbikxxkYz1sb2NhbC1sInIYmply3Rfcmdhbm1eYXRpb24icolsiRxhhhXbsZSB
Pcmdhbm1eYXRpb241XSwcmwes2Xh1o1siQ2xpmb1jYWxB2Glpbm1zdHJhdg9ycyis1KnvbhR1bn
R2Zdpbm1zdHJhdg9ycyis1InSc3R1bUFkbW1uaXNucmFB3j2t10e1InIYmply3RS8C2x1fjpbe
yvjb2R1tjoiQ2xpmb1jYWxB2Glpbm1zdHJhdg9ycyis1mNvZGVTeXN0Z01oiIXLjMUN4xLjou
M840MDM3Ns4yljExujEf8x7mNvZGU10i2Db250ZW5QRTaw5pc3YXvcmnIlCjzb2R1U1
zdgVtjoiM84zLjYm840UjEuNDa2zEuMi4xM4xIn0seyyjbcR1tjoiU31zdgtvCWRtaW5pc3
FYXvcmnIlCjzb2R1U1zdgtvCtjo1Ms4zLjYm840LjEuNDa2zEuMi4xM84xrnldCjgdokio
ivjOXLG72yRVBQ110ajhRcvBhHZB1iwiwF0UjoxNjk4NDc40TA3LCJ1eHa1OjE207gwRzkY
Mdcsim51zil6MTY5ODA3ODYWN30.pdfIm6R3x3pREbbyW4x56UD6ocLCHD9eSiUv-TvD0uzv
F99BC3R0h1DOKWIGzh_91YvWb1aPVXkb8QXqguo2tEPje9rHoy78yYIqQ2gft2zPipHov-yja
KX6EqFftoytFvW3jh16GDgbgy6crpjYq2FRac7dHKghKbnccctm_mPgItO_EE0UsaL87LsCNI
X08tt5uvZYWS8F2tq-1bbzD0LyQzvSpbQLbxzw_ueC_DbtRqV263c2zCoash0-huMrwXpBItvl
2B6odgi7QwWjzqzPAyy0l0enux1sVt4IAczaaD8PsyIwm6EFWPjVcv_KG9NoubNqli7yw
9 Content-Type: application/x-www-form-urlencoded
10 X-Requested-With: XMLHttpRequest
11 Dnt: 1
12 Referer:
https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/admin/overview.html

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Target: <https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com>

```

Request
Pretty Raw Hex
1 GET /admin/services/admin/components/workflow/status/retrieve.json?format=
true HTTP/2
2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
3 Cookie: JSESSIONID=B4ABC6143974B3010830317ABD1F3B9
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/118.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 X-Requested-With: XMLHttpRequest
0 Dnt: 1
1 Referer:
https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/admin/o/
view.html
2 Sec-Fetch-Dest: empty
3 Sec-Fetch-Mode: cors
4 Sec-Fetch-Site: same-origin
5 Sec-Gpc: 1
6 Te: trailers
7
8

Response
Pretty Raw Hex Render
1 HTTP/2 401 Unauthorized
2 Content-Type: application/json;charset=UTF-8
3 Date: Mon, 23 Oct 2023 16:39:02 GMT
4 Forcare.com-Logcontext: f90178012241/admin-111417
5 Vary: accept-encoding
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: SAMEORIGIN
8 X-Xss-Protection: 1; mode=block
9 Content-Length: 356
10
11 {
12   "message": "authentication required",
13   "logContextId": "f90178012241/admin-111417",
14   "origin": "/admin/services/admin/components/workflow/status/retrieve.json"
15   ,
16   "causes": [
17     "nl.forcare.common.servlet.HttpErrorException: authentication required"
18   ],
19   "stacktrace": [
20     {
21       "text": "nl.forcare.common.servlet.HttpErrorException: authentication required"
22     }
23   ]
24 }
25

```

Once the Token is expired, when we send the retrieve.json request that also gives the 401 unauthorized error message, hence this case 1 is fixed.

## Case 2:

Step1: Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Capture this request(<https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/services/admin/components/admin/config/properties.json>) and send to repeater

Step3: Logout from Admin account

Step4: Now capture the cookies and tokens of Viewer and Audit account replace with admin cookies and tokens and forward the request

Step5: You can see that Viewer and Audit users can view the admin properties.

## Supported Evidences:

Actual request from Admin:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Modified request with Viewer and Audit cookies and tokens.

## **Retest (02-Jun-2023):**

## Case1:

The steps same as before

## Case2:

**Step1:** Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Leave the setup idle for about 5-10mins, the token becomes unauthorized.

Step3: Send the retrieve data request to repeater and observe the behavior.

### **Supportive Evidence:**

### Case1:

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Three screenshots of a browser-based security testing interface showing requests and responses for two different URLs.

**Screenshot 1 (Top):** Request URL: <https://10.196.27.233>. Response URL: <https://10.196.27.233/admin/services/admin/components/connect/config/properties.json>. The response body contains several sensitive configuration parameters highlighted with a red box, including:

```

    "properties": {
        "forceHTTPS": "true",
        "properties": {
            "dbDriver": "org.postgresql.Driver",
            "properties": {
                "url": "jdbc:postgresql://localhost:5432/forcare",
                "username": "forcare",
                "password": "forcare"
            }
        },
        "indexOn": "https://localhost:8083/index",
        "properties": {
            "ESIndexName": "IntelliSpace_Echange",
            "ESIndexType": "string"
        }
    }
  
```

**Screenshot 2 (Middle):** Request URL: <https://10.196.27.233>. Response URL: <https://10.196.27.233/admin/admin/overview.html>. The response body contains sensitive configuration parameters highlighted with a red box, including:

```

    "properties": {
        "viewURL": "https://localhost:8083/view",
        "properties": {
            "viewType": "local",
            "properties": {
                "url": "http://localhost:8083/forcare/default"
            }
        }
    }
  
```

**Screenshot 3 (Bottom):** Request URL: <https://10.196.27.233>. Response URL: <https://10.196.27.233/admin/admin/overview.html>. The response body contains sensitive configuration parameters highlighted with a red box, including:

```

    "properties": {
        "viewURL": "https://localhost:8083/view",
        "properties": {
            "viewType": "local",
            "properties": {
                "url": "http://localhost:8083/forcare/default"
            }
        }
    }
  
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## Case2:

## Old POC:

1. Configure your browser to use a proxy tool such as Burp.
  2. Log in to the forcare admin application as user without SYSTEM\_PHI\_READ.
  3. It is observed that the user without SYSTEM\_PHI\_READ role defined can view/read the following api endpoints which consists of sensitive information like, backend components/versions, encryption password etc.

### **Supportive Evidence:**

A user with SYSTEM\_PHI\_READ has view option on backend configuration which includes sensitive information.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Target: <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com>

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	<ul style="list-style-type: none"> <li>Request Attributes</li> <li>Request Query Parameters</li> <li>Request Body Parameters</li> <li>Request Cookies</li> <li>Request Headers</li> <li>Response Headers</li> </ul>
<pre>1 GET /admin/services/admin/components/viewer/config/properties .json HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=D3B98FC44FAED2F73A9DE7379339C7 4 Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99" 5 Content-Type: application/x-www-form-urlencoded 6 X-Requested-With: XMLHttpRequest 7 Sec-Ch-Ua-Mobile: ?0 8 Authorization: Bearer eyJhbGciOiJSUzIiNiImlingIdCI6IjFLbmQtSER4eEgtZkZjeX1xBylDT mpnVVFCyJ9..eyJpc3MiOiJlcm4eBz1kCjEuM140IiwiYXVkjoiiaHR0c HMELYsb2NhbGhvC3Q6ODA4MS92aW3ZX1LCJzdWIiOiJyb390IiwiU3 ViamVjdlEIjoicm9vdCIiKhnbm9uaWNhbFVzZXJJZC16InVpZDiyb29 OLGRjPWRvWFpbixK7zimb2NhbC1sI1NIYmLY3Rcmdhbml6YXpb241 O1s1RxbhXBSpmdhbml6YXpb241XSwicms9ZXMiolsiQ2xpbnljiY WxBZGphmlzdHJhdG9ycyilb1N5c3RlbUFkbWluuXNOcmF0b3zil0s1l N1Ymp1Y3RSb2x1jpbeuyjb2R1ljoiQ2xpbmjiYWxBZGphmlzdHJhdG9 ycylsImhVZGVTeXN0ZD01O1IxLjMuN14xLjQuHS40MDM3MS4yLjExiJE1 ESX7ImNvZGU1o1JteXN0ZW1BZGipbmlzdHodG9ycylsImhVZGVTeXN0Z W010i1xljMuN14xLjQuHS40MDM3MS4yLjExLjEifV0oas161jBHW V2SKRVQ05mxzYvVtxUvg4QkE1LCJpYXQiOjE2NsUaNjA0NsEsImV4cCI eMTY3NTE2MDc3MSwibmjmIjoxNjciMTYwMTcxQ.QvQv29LQVXG9w1-o QbyxCkewUhkx6el52ITptrOjuzuGMrRt3iTcq46t601NE-tgF3Ku5m uloEb24rdMNsAOFMV3tFKErzQzH7vDMMWhR0KEn...eBjXKp4Ez9Ug61Sc0 1Lfrf4d4nnccm1Ma8T7uaf1ivnmcrafxV1na4DNkTSvrxnh.BMHT7rTx33Ym</pre>	<ul style="list-style-type: none"> <li>Request Attributes</li> <li>Request Query Parameters</li> <li>Request Body Parameters</li> <li>Request Cookies</li> <li>Request Headers</li> <li>Response Headers</li> </ul>	

Target: <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com>

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	<ul style="list-style-type: none"> <li>Selection</li> <li>Selected text           <pre>forcare</pre> </li> <li>Request Attributes</li> <li>Request Query Parameters</li> <li>Request Body Parameters</li> <li>Request Cookies</li> <li>Request Headers</li> <li>Response Headers</li> </ul>
<pre>1 GET /admin/services/admin/components/admin/status/status.js on?format=true HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=BAA55128FOAF1440AA0ASEC6336A2E 4 Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99" 5 Content-Type: application/x-www-form-urlencoded 6 X-Requested-With: XMLHttpRequest 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/109.0.5414.75 Safari/537.36 9 Sec-Ch-Ua-Platform: "Windows" 10 Accept: /* 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer:   https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.c om/admin/admin/overview.html 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Connection: close 18 19</pre>	<pre>834  { 835   "key": "package.access", 836   "value": "sun.org.apache.catalina.,org.apache.coyote., org.apache.jasper.,org.apache.tomcat." 837 }, 838   "key": "server.loader", 839   "value": "" 840 }, 841   "key": "forcare.passwordEncryptionKeyStorePassword", 842   "value": "forcare" 843 }, 844   "key": "forcare.passwordEncryptionKeyStoreUrl", 845   "value": "file:/usr/local/forcare/certificates/password encryption.p12" 846 }, 847   "key": "forcare.configproperties.ISPtls", 848   "value": "false" 849 }, 850   "key": "forcare.configproperties.ISPtls", 851   "value": "false" 852 }, 853 }</pre>	<ul style="list-style-type: none"> <li>Selection</li> <li>Selected text           <pre>forcare</pre> </li> <li>Request Attributes</li> <li>Request Query Parameters</li> <li>Request Body Parameters</li> <li>Request Cookies</li> <li>Request Headers</li> <li>Response Headers</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



### 8.3 Webapp: Weak Password Policy

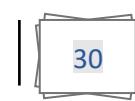
Vulnerability Title	Weak Password Policy
Vulnerability Category	A6 - Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.6 CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:N
Description	<p><b><u>Vulnerability Description:</u></b></p> <p>The application does not enforce a strong password policy to prevent malicious users from manually guessing or brute-forcing legitimate account passwords. Weak password policies include those that allow passwords consisting of common dictionary words, commonly-used passwords (For example., 1234), passwords that contain the associated username, sequential characters, and passwords shorter than 9 characters. By allowing users to create easily-guessable passwords, an attacker with minimal knowledge of registered users and username formats could crack passwords through the use of any of several techniques. In an online attack, an attacker can use consecutive login attempts to determine simple passwords. In an offline attack (For eaxmple., if the attacker has gained access to the raw contents of the password database through some other means), the attacker can employ richer techniques such as pre-computed hash attacks, free of rate-limiting and account-locking protections that might be employed against online password brute-forcing attacks.</p> <p><b>Retest (23-Oct-2023):</b> Issue exists in retest, no password policy in place.</p> <p><b>Exploitability rational:</b> Weak passwords may be easily guessed. This increases the likelihood a user's account may be compromised by an attacker. Once compromised, an attacker can have full access to the victim's account, potentially including the ability to modify settings, features and passwords. If the target account holds administrative privileges, the attacker can modify data for other users and/or the entire system.</p> <p><b>Impact Rational:</b> Credentials can be easily brute force. . Due to the prevalence of password reuse, a compromised password may also provide an attacker with</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	credentials that can be used to attack other systems the victim uses the same credentials to access.
Affected Systems/IP Address/URL	<p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a></p> <p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a></p> <p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a></p> <p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload</a></p>
Recommendation	<p><b>Recommendation:</b></p> <p>Implement a strong password complexity policy. A strong password policy is one which combines rules to prevent easily guessable passwords from being used while also ensuring that passwords contain sufficient entropy. A password policy which provides a large set of restrictions can ultimately result in a smaller potential pool of passwords, lowering the amount of time necessary to guess a password through brute-force attacks. Conversely, an overly permissive policy allows users to create easily guessable passwords. Put constraints in place to prevent users from choosing easily guessable passwords at the time of creation, specifically those that are targeted by well-known dictionary attacks. This can minimize the likelihood that an attack may be successful if an attacker attempts to guess commonly used passwords or employs an automated dictionary attack against a particular user.</p> <p>In the event that company policy does not stipulate password requirements, or the existing requirements are weak, consider employing the following password complexity requirements:</p> <ul style="list-style-type: none"> <li>• Passwords must be at least nine (9) characters long.</li> <li>• Passwords must contain some combination of at least three (3) of the following classes of characters: lowercase, uppercase, numeric, and “special” (For example., !, @, #, \$, %, ^, etc.) characters.</li> <li>• Passwords should not be a dictionary word in any language, slang, dialect, jargon, etc.</li> <li>• Passwords should not be based on personal information, etc.</li> </ul>
Status	OPEN



## Steps to Reproduce:

### Retest (23-Oct-2023):

Steps to Reproduce:

Step1: Login to Admin account

Step2: Navigate to home -> User Management -> Users -> New User

Step3: Provide all the mandatory details (eg: im creating an account with Test1234/ Test1234 weak password)

## Supported Evidences:

```

https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com POST /admin/services/user/add ✓ 200 365

```

Request		Response
Pretty	Raw	Raw
Hex		
<pre> 9 Authorization: Bearer eyJhbGciOiJSUzIiInIidC16IjJlbmQtsSR4eEgt2kZjeXlXby1D7mpn0VVFCyJ9.eyJpc3MiOiJlc46b2lkOjEuMj40IiwiYXVkiJoiaHR0cHM6Ly9sb2Nhbsghvc306ODA4MS92aWV3ZXiiLCJzdwIi0iJyb29UiwiU3VlamVjdElEijoicm9vdCisIkNhb9uaWNhbFVzZKXJC16InVpZD1ybh29ULGRjPWRvbWPbiixkYz1sb2NhbcIisI1N1YmplY3RPcmdhba6YXRpb24i0ls1RxbhbXBeZSBPcmdhbm16YXRpb24iXSwlcm9sZXMiOlisiQ2xpbljYWx8ZGlpbmldhJhdG9ycyIsI1N5c3R1bUFkbWluaxN0cFOb3zz10sI1N1YmplY3Rsb2xlIjpbeyjzb2R1i0iQ2xpbljYWx8ZGlpbmldhJhdG9ycyIsI1NvZGVTeXn0ZW0i0itxLjMuNi4xijQuMS40MDM3MS4yLjExljRif5x7imNzGUoiidBc2502W5D0WRtaW5pc3RyYXRvcnMiLCJjb2R1U31zdGvtIjoiMS4zLjYuMS40LjEuNDazN2EuNi4xMs4xIn1dLCJqdGkiOjJHmhgbTNSM51tUiwUdWQUFaER311wiaWP0ijoNxNjk4MDgyMjMzLCj1eHAi0jE20rgwUD1IMzMs1m5i21IGMTY50DA4MTkzM30_pjrbpVZq8_wk2ZIKvOVOJaiPW_Lbqsv7dcany5hle02vW-o-xDUYg_yGokw63xTQVCquchsawx9nU31rpQuqxutBUbv35Y0ctmPLGgWcRQXFb-PcQH5tO7vpv8sUKCNkI0dt73NDTtQ6oHtpZsQhc6f60szal1hBycoWb7af-8zeCCDFIBmeqKeko9iNmIN_KheqgTRLAG2ps-UPSi1ErfdxEq9nvNKGHwgEpdUYTdswmTp3Gmc4mKa2swJX12vbh12iyXU04cBfRLBf0nNmLEAvemD0uqYrOY8N5sbj44D3XW_TOoQwa_0hK_AXQ </pre>		<pre> 1 HTTP/2 200 OK 2 Cache-Control: no-store,    no-cache,    must-revalidate 3 Cache-Control: post-check=0,    pre-check=0 4 Content-Type: application/octet-stream 5 Date: Mon, 23 Oct 2023    17:32:42 GMT 6 Expires: 0 7 Forecare.com-Logcontext: f90178012241/admin-112167 8 X-Content-Type-Options: nosniff 9 X-Frame-Options: SAMEORIGIN 10 X-Xss-Protection: 1;    mode=block 11 Content-Length: 0 12 13 </pre>

### Retest (05-Jun-2023):

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## Old POC:

Weak password accepted for add user feature in ForAdmin portal.

The screenshot shows the Postman interface with three panels: Request, Response, and Inspector.

**Request:**

- Pretty
- Raw
- Hex

1 POST /admin/services/user/add HTTP/1.1  
2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com  
3 Cookie: JSESSIONID=13E603293D34C973F239EA861CCCE66  
4 Content-Length: 276  
5 Sec-Ch-Ua: "Chromium";v="109", "Not\_A\_Brand";v="99"  
6 X-Forcage-Challenge: [REDACTED]  
7 Sec-Ch-UA-Mobile: ?0  
8 Authorization: Bearer [REDACTED]  
9 Connection: close  
10  
11 uid=1&email=1401.com&givenName=a&sn=a&cn=a&postalAddress=a&userPassword=ad0=Hestia%20General%20Practitioners&ou=Hestia%20General%20Practitioners&organizationUnit=hestia.general.practitioners&telephoneNumber=&mobile=&pager=&registeredAddress=&title=&initials=&preferredLanguage=

**Response:**

- Pretty
- Raw
- Hex
- Render

1 HTTP/1.1 200 OK  
2 Cache-Control: no-store, no-cache, must-revalidate  
3 Cache-Control: post-check=0, pre-check=0  
4 Content-Length: 0  
5 Content-Type: application/octet-stream  
6 Date: Mon, 30 Jan 2023 06:21:45 GMT  
7 Expires: 0  
8 Forcage.com-Logcontext: f90178012241/admin-573280  
9 X-Content-Type-Options: nosniff  
10 X-Frame-Options: SAMEORIGIN  
11 X-Xss-Protection: 1; mode=block  
12 Connection: close  
13  
14

**Inspector**

- Request Attributes
- Request Query Parameters
- Request Body Parameters
- Request Cookies
- Request Headers
- Response Headers

Weak login password for the portals.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.4 Webapp: DOM Cross-Site Scripting (XSS)

Vulnerability Title	DOM Cross-Site Scripting (XSS)
Vulnerability Category	A3- Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment it is observed that the application is vulnerable to DOM XSS attack.</p> <p>DOM based XSS is an XSS attack wherein the attack payload is executed as a result of modifying the DOM “environment” in the victim’s browser used by the original client-side script, so that the client-side code runs in an “unexpected” manner. That is, the page itself (the HTTP response that is) does not change, but the client-side code contained in the page executes differently due to the malicious modifications that have occurred in the DOM environment.</p> <p><b>Retest (23-Oct-2023):</b> Issue fixed in retest</p> <p><b>Exploitability Rational:</b> For a successful exploitation of the issue, the victim should not be logged in to the application.</p> <p><b>Impact Rational:</b> DOM Cross-Site Scripting vulnerabilities give the attacker control of HTML and JavaScript running the user’s browser. The attack can alter page content with malicious HTML or JavaScript code. The attacker can arbitrarily alter page content displayed to the victim and can execute application functions using the victim's application identity if the victim is authenticated to the application.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/patient/query:_global!">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/patient/query:_global!</a>
Recommendation	It is recommended to have proper input validation, also checking syntax semantic (For example, a name field allowing special chars, number field accepting anything other than numeric digits., or allowing custom URL schema).

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<p>Validation at Server side is required, you can bypass client side within JavaScript.</p> <p>Encode the output with Encoder.encodeForHTML and Encoder.encodeForJS before making dynamic updates to HTML.</p> <p>Considering any form of user input as untrusted and sanitizing it before operating anywhere.</p> <p>Avoid methods such as document.innerHTML and instead use safer functions, for example, document.innerText and document.textContent. If you can, entirely avoid using user input, especially if it affects DOM elements such as the document.url, the document.location, or the document.referrer.</p>
Status	<b>CLOSED</b>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Steps to Reproduce:****Retest (23-Oct-2023):****Supportive evidences:**A screenshot of a web browser displaying the 'HealthSuite Interoperability Viewer' patient search interface. The URL in the address bar is https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/patient/query\_global. The main page shows fields for 'Last Name', 'Given Name', 'Patient ID', 'Name', 'Date of Birth', and 'Gender'. Below these are dropdowns for 'HOS: Hospital' and 'Date of Birth (m/d/yyyy)', and radio buttons for 'Male', 'Female', and 'All'. On the left, there's a 'Restrict query' section with dropdowns for 'anywhere' and 'with or without documents', and buttons for 'Reset' and 'Search'. A green button labeled 'Show referrals' is also present. A modal dialog box is overlaid on the page, containing a large red 'X' icon, the text 'Something went wrong', and the message 'malformatted request: no wildcards permitted in patientID'. It also includes a link 'Additional information can be found in [forAdmin](#)'. At the bottom right of the modal is a blue 'OK' button.**Supportive evidences (03-Jun-2023):**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The screenshot shows a web browser window for the HealthSuite Interoperability Viewer. The URL in the address bar is [https://3.71.200.223/viewer/document/list.html?patientID=<img%3c%3dx%20onerror%3daudit\(document.URL\)>%5E%5E%201.3.6.1.4.1.21367.2005.3.78150#0/document/container/medicalDocuments/patientId=%20&%3Bimg%2fsrc%3D%20onerror%3Dalert%28document...](https://3.71.200.223/viewer/document/list.html?patientID=<img%3c%3dx%20onerror%3daudit(document.URL)>%5E%5E%201.3.6.1.4.1.21367.2005.3.78150#0/document/container/medicalDocuments/patientId=%20&%3Bimg%2fsrc%3D%20onerror%3Dalert%28document...). The page displays a search interface for medical documents, with tabs for Medical Documents, Referrals, Patient Consent, Patient Details, and Exports. A prominent red-bordered dialog box is centered on the screen, containing an error message and technical details.

**Filter results:** No documents | Change purpose of use

**Creation Date:** Title | **Author Role:** Author Institution: Type:

**Something went wrong**

nl.formare.xds.util.XdsException: ERROR; errorCode: XDSRegistryMetadataError; codeContext: metadata.error((registry)); Could not parse the request. Reason: com.sun.xml.bind.v2.runtime.IllegalAnnotationsException: 1 problem was detected.  
onerror=&gt;<img%3c%3dx%20onerror%3daudit(document.URL)>%5E%5E%201.3.6.1.4.1.21367.2005.3.78150#0; cause &lt;img%3c%3dx%20onerror%3daudit(document.URL)>%5E%5E%201.3.6.1.4.1.21367.2005.3.78150#0; is not a valid patient ID in XDS; format should be id="^a&authority#&id0; location: ParseError

- ERROR; errorCode: XDSRegistryMetadataError; codeContext: metadata.error((registry)); Could not parse the request. Reason: cannot parse patient ID. The XML is invalid.

**OK**

## **Supportive evidences:**

**Payload:** <img/src%3dx%20onerror%3dalert(document.URL)>

A screenshot of a Microsoft Edge browser window. The address bar shows a URL: "https://modern-cougar.aws.pentest forcarelabs.com/viewer/document/list.html?patientID=<img src%3d onerror=alert(document.URL)%3E%5E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO". A red box highlights this URL. Below the address bar, a dark gray warning dialog box is displayed. The dialog has a white background and a black border. It contains the text "⊕ modern-cougar.aws.pentest forcarelabs.com" and a long URL. The URL is: "https://modern-cougar.aws.pentest forcarelabs.com/viewer/document/list.html?patientID=%3Cimg%0A/src%3d%20onerror%3Daler%28document.URL%29%3E%5E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO". At the bottom right of the dialog is a blue "OK" button. The entire dialog is also enclosed in a red box.

## **Retest (31-Jan-2023):**

Throws uncaught exception error which indicates the fix is not implemented properly.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Screenshot of the HealthSuite Interoperability Viewer showing a security error. The URL is https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/document/list.html?patientID=<img/src%3dx%20onerror%3daler... . The page displays a 'Something went wrong' message with a red X icon. The error message is: n!forcare.xds.util.XdsException: ERROR; errorCode: XDSRegistryMetadataError; codeContext: metadata error (registry): Could not parse the request. Reason: cannot parse patient ID: &lt;img/src=x onerror=alert(document.URL)&gt; (&lt;img/src=x onerror=alert(document.URL)&gt;)^~^&lt;1.3.6.1.4.1.21367.2005.3.7&ISO: is not a valid patient ID in XDS; form should be id^^^&authority&ISO.; location: ParserUtil.handleMetadataError . An 'OK' button is at the bottom right of the error dialog.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.5 Webapp: Weak Input Validation

Vulnerability Title	Weak Input Validation
Vulnerability Category	A3 - Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L
Description	<p><b>Vulnerability Description:</b> During the assessment it is observed that the application stores or processes untrusted data that is not sufficiently validated. This may be due to a complete lack of validation or validation filters whose implementation does not provide sufficient protection for the given input. An application may obtain data from various external and internal sources including databases, file servers, web services, external client requests, etc. While some of these sources may be considered trustworthy, no assumptions should be made about the validity of data whose source cannot be explicitly verified. This includes not only external data, but also data that was previously stored by the same application and data generated by other entities in the same organization.</p> <p><b>Retest (23-Oct-2023):</b> Issue exists in retest.</p> <p><b>Exploitability Rational:</b> Failure to properly validate and handle untrusted input represents the single largest category of software security weaknesses. At a minimum, data that is not validated may impact the application's control flow or data flow, leading to unexpected application states for end users, unintended changes to back-end data, as well as unexpected outcomes from executed application logic.</p> <p>An attacker may submit payloads that seek to exploit any number of vulnerabilities that typically result from a lack of input validation. These include (but are not limited to) SQL injection, cross-site scripting, LDAP injection, log injection, and command injection. The consequence of successfully exploiting these vulnerabilities varies, but most provide an attacker with the ability to bypass authentication and/or authorization mechanisms to access, modify or delete application and user data, or execute functionality only available to legitimate users.</p> <p><b>Impact Rational:</b> An attacker can provide unexpected values and cause a program crash or excessive consumption of resources, such as memory and</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	CPU. An attacker can read confidential data if they can control resource references. An attacker can use malicious input to modify data or possibly alter control flow in unexpected ways, including arbitrary command execution.
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a>
Recommendation	We recommend the following: <ul style="list-style-type: none"><li>• Data that does not match an expected pattern and data that can potentially be used to execute injection attacks must be discarded or sanitized before use.</li><li>• Perform the validation in such a way that end-users cannot tamper with or bypass the control. Perform the validation on the server-side rather than client-side.</li></ul> Whitelist validation should be favored first over other validation techniques since any character or string not explicitly specified as part of the "known-safe" set of characters or values is rejected or removed by default.
Status	OPEN

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



### Steps to Reproduce:

### Supportive evidence:

### Retest (23-Oct-2023):

HealthSuite Interoperability Viewer

Home > Patient Search > Patient Record > Medical Documents

<script>alert(1)</script>, <script>alert(1)</script>	ID: <script>alert()</script> (ISX)	Jan 1, 2011 (12 yr)	Male
Address <script>alert(1)</script>, 234567 <script>alert(1)</script>	Phone -	Email -	

Medical Documents Referrals Patient Consent Patient Details Exports

Filter results: No documents

Add a document

Creation Date ▾ Title ▾ Author ▾ Author Role ▾ Author Institution ▾ Type ▾

### Retest (06-Jun-2023):

HealthSuite Interoperability Viewer

Home > Patient Search > Patient Record > Medical Documents

<h1>lastName</h1>, <h1>givenName</h1>	ID: <h1>myID</h1> (HOS)	Aug 9, 2010 (12 yr)	Male
Address <h1>Street</h1>, <h1>postalcode</h1> <h1>resident</h1>	Phone -		

Medical Documents Referrals

Filter results: No documents | Change purpose of use

Select all No actions applicable

Creation Date ▾ Title ▾ Author ▾ Author Role ▾ Author Institution ▾ Type ▾

### Old POC:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Screenshot of the HealthSuite Interoperability Viewer interface showing a patient record. A red box highlights the address field containing the value '<h1>pentest</h1>, <h1>pentest</h1>'. The interface includes a navigation bar, patient details (ID: 102 (HOS), Jan 1, 2022 (1 yr), Male), and tabs for Medical Documents, Referrals, Patient Consent, Patient Details, and Exports. The Medical Documents tab is selected.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.6 Webapp: Improper Error & Exception Handling

Vulnerability Title	Improper Error & Exception Handling
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS v3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> it is observed that the web application reveals sensitive information as part of its error messages such as stack trace, server versions, name of server-side parameter.</p> <p><b>Retest (23-Oct-2023):</b> Issue exists in retest</p> <p><b>Exploitability Rational:</b> An attacker does not require authentication to the platform in order to leverage this vulnerability.</p> <p><b>Impact Rational:</b> Attackers may use this vulnerability to gain more information about the system before attempting to attack the web application.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a>
Recommendation	It is recommended to Implement a mechanism to handle and log all errors that pull out the exception stack trace message. It is also recommended to display a generic error message instead of the stack trace.
Status	Open

### Steps to Reproduce:

Retest (23-Oct-2023):

### Supportive evidences:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## **Retest (06-Jun-2023):**

Old:

Improper error and exception as part of server response.

Send Cancel < > Search... 0 matches

Target: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com

Request	Response	Inspector
<p>Pretty Raw Hex</p> <p>1 POST /audit/services/audit/list.csv HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: center_bottom; JSESSIONID=0177BEEB1348C44B0B95F444F5B3ACD8 4 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99" 5 Sec-Ch-Ua-Mobile: 20 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: iframe 14 Referer: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit/index.html 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9</p>	<p>Pretty Raw Hex Render</p> <p>1 HTTP/1.1 405 Method Not Allowed 2 Content-Type: text/xml;charset=UTF-8 3 Date: Mon, 30 Jan 2023 05:18:27 GMT 4 Forcare.com-Logcontextid: a8ac19a8a030/audit-119391 5 Vary: accept-encoding 6 X-Content-Type-Options: nosniff 7 X-Frame-Options: SAMEORIGIN 8 X-Xss-Protection: 1; mode=block 9 Content-Length: 6032 10 Connection: close 11 12 &lt;error message="POST method not allowed for path /services/audit/list.csv" logContextId="a8ac19a8a030/audit-119391" origin="#" /audit/services/audit/list.csv"&gt; 13 &lt;cause&gt; 14 &lt;cause&gt;nl.forcare.common.servlet.HttpErrorException: POST method not allowed for path /services/audit/list.csv &lt;/cause&gt; 15 &lt;/cause&gt; 16 &lt;stacktrace&gt; nl.forcare.common.servlet.HttpErrorException: POST method not allowed for path /services/audit/list.csv at nl.forcare.frontcontroller.MappingUrlMapper.createHandler 17</p>	<p>Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers</p>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



The screenshot shows the Network tab of a browser developer tools interface. A red box highlights the URL of a successful GET request to `/admin/services/admin/queue/retrieve.json?id=1`. Another red box highlights the error message in the response body: `Apache Tomcat/9.0.68`.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



## 8.7 Webapp: Sensitive Information in the URL

Vulnerability Title	Sensitive Information in the URL
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment, it is observed that Sensitive information is exposed in via URL query string parameters. Username, PatientID, userID, Code are exposed via URL parameters. URLs may be stored or viewed in multiple places during and after a request is made to the server:</p> <ul style="list-style-type: none"> <li>URLs are often logged in multiple places including the browser history, proxy logs, and web server logs.</li> <li>The query string will be sent as part of the URL if the URL is passed to another site via the Referrer header.</li> <li>URLs sent to the user as part of an HTML page may be cached on disk.</li> </ul> <p><b>Retest (23-Oct-2023):</b> Issue exists in Retest.</p> <p><b>Exploitability Rational:</b></p> <p>Potential access vectors may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>Browser history, proxy logs, web server logs, etc.</li> <li>Utilizing other attacks (such as cross-site scripting) to extract sensitive information from the source of a page containing links to URLs with sensitive information in the query string</li> <li>Shoulder-surfing the URL in a user's browser address bar.</li> </ul> <p><b>Impact Rational:</b> Attacker who gains access to any location where URLs are stored can view sensitive information passed via the query string. Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which would allow user impersonation (in the event of credential or session identifier).</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/services/document/list.json?patientID=356924500&amp;patientIDAuth=1.3.6.1.4.1.21367.2005.3.7">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/services/document/list.json?patientID=356924500&amp;patientIDAuth=1.3.6.1.4.1.21367.2005.3.7</a>
Recommendation	Do not pass the sensitive data like credentials, UserID, codes or sessionIDs between the client and server via URL query string parameters.
Status	OPEN

### Steps to Reproduce:

**Retest (23-Oct-2023):**

### Supported evidences:

#	Host	Method	URL	Params	Edit
6708	https://ec2-3-71-200-223.eu... GET	/viewer/services/document/list.json?patientID=356924500&patientIDAuth=1.3.6.1.4.1.21367.2005.3.7			✓
<b>Request</b> <a href="#">Pretty</a> <a href="#">Raw</a> <a href="#">Hex</a>			<b>Response</b> <a href="#">Pretty</a> <a href="#">Raw</a> <a href="#">Hex</a> <a href="#">Render</a>		
1	HTTP/2 200 OK				
2	Cache-Control: no-store, no-cache, must-revalidate				
3	Content-Type: application/json; charset=UTF-8				
4	Date: Mon, 23 Oct 2023 18:03:21 GMT				
5	Expires: 0				
6	Forcare.com-Logcontext: 79abf00le495/viewer-36530				
7	Vary: accept-encoding				
8	X-Content-Type-Options: nosniff				
9	X-Frame-Options: SAMEORIGIN				
10	X-Xss-Protection: 1; mode=block				
11	Content-Length: 10713				
12	{				
13	"result": { "warnings": [ ], "documents": [ { "mimeType": "application/pdf", "id": "fc378770-ec9c-4b6e-bea6-74e1237d9f59", "logicalId": "fc378770-ec9c-4b6e-bea6-74e1237d9f59", "status": "Approved", "objectType": "STABLE_DOCUMENT", "home": "1.2.3", "creationTime": "19960331", "hash": "a1fe7f3900b18c027a5bc8cd17a416b3d57b526", "languageCode": "en-US", "repositoryUniqueId": "1.2.3", "serviceStartTime": "19960331", "serviceStopTime": "19960331", "size": "64698", "sourcePatientId": "356924500^^^BSN"         }       ]     }				
14	]				

**Retest (06-Jun-2023):**

Steps are same as before.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Request

```
Pretty Raw Hex
1 GET /viewer/services/document/list.json?patientID=734524500&patientIDAuth=
2 [REDACTED] 1.3.1.21367.2005.3.7 HTTP/1.1
3 Host: 3.71.200.223
4 Cookie: JSESSIONID=DAB4444E191E00BAA7605A118F50
5 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99"
6 Content-Type: application/x-www-form-urlencoded
7 X-Requested-With: XMLHttpRequest
8 Sec-Ch-Ua-Mobile: ?
9 Authorization: Bearer
eyJhbGciOiJSUzInIiInIisInIdCI6IjFlbmQtSER4eEgtZkZjeXl
Xby1DTmpnOVVFcyJ9.eyJpc3MiOiJlcjm46b2lkOjEuM140IiwiY
XVkijoiaHR0cHM6Ly5b2NhbGhvC3Q6D0A4MS92aWV3ZXiiLCJz
dWIiOjybj290IiwiU3ViamVjdE1Eijoicm9vdCisIkNbhsQuaWN
hbFvZ2XJJZCIEInVp2Dlyb290LGRjPWRvbWPpbixkYz1sb2Nhbc
ISiIN1Ymp1Y3RFcmdbmleYXRpb24iOlsirXkbhXBsZSBPcmdb
m16YXRpb24iXSwicm5sZXMiOlsQ2xpblmjYWxBZGlpbmlzdHjh
dG9ycyIsIiIN5c3R1bUFkbWuaXN0cmFOb3JzI10sIiIN1Ymp1Y3R
Sb2x1IjpbeYjb2R1Ijo1Q2xpblmjYWxBZGlpbmlzdHjhG9ycy
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Type: application/json; charset=UTF-8
5 Date: Mon, 30 Jun 2023 13:21:27 GMT
6 Expires: 0
7 Forcare.com-Logcontext: 79a0f001e495/viewer-4350
8 Vary: accept-encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Xss-Protection: 1; mode=block
12 Content-Length: 9996
13 Connection: close
14
15 {
  "result": [
    {
      "warnings": [
        {
          "document": {
            "id": "fc78770-e9c-48e-7e1237d9f59",
            "loginalid": "c137870-ecb-4be-bead-74e1217d8f59",
            "name": "John Doe",
            "objectType": "STABLE_DOCUMENT",
            "home": "+1.2.3.",
            "logonTime": "19900311",
            "hash": "1a127f1900010c027a5bc0d17a41b3d57b526",
            "languageCode": "en-US",
            "referenceTime": "19900311T12:37",
            "serviceStartTime": "19900311",
            "serviceStopTime": "19900311",
            "source": "Patient ID: 134024500***41.3.6.1.4.1.21367.2005.3.74190",
            "sourcePatientInfo": [
              {"id": "fc78770-e9c-48e-7e1237d9f59", "version": "1.3.6.1.4.1.21367.2005.3.74190", "pid": "51Atweig9Geric", "pid7": "19671111", "pid8": "01-R"}, {"id": "fc78770-e9c-48e-7e1237d9f59", "version": "1.3.6.1.4.1.21367.2005.3.74190", "pid": "51Atweig9Geric", "pid7": "19671111", "pid8": "01-R"}]
        }
      ]
    }
  ]
}
```

Inspector

- Request attributes: 2
- Request query parameters: 2
- Request cookies: 1
- Request headers: 17
- Response headers: 12

## Old POC:

- Launch ForView Applications.
- Intercept the requests using Burp proxy tool.
- As observed in below request PatientID and PatientIDAuth value gets sent for GET requests, which can get logged.

Request

```
Pretty Raw Hex
1 GET /viewer/services/domain/list.json
2 [REDACTED] https://ec2-3-70-166-239.eu-ce... GET /viewer/services/document/list.json?patientID=7345342758955&patientIDAuth=[REDACTED] 1.3.6.1.4.1.21367.2005.3.7 HTTP/1.1
3 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com
4 Cookie: JSESSIONID=18E4C3E3306978427688E8F51FF5E97
5 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99"
6 Content-Type: application/x-www-form-urlencoded
7 X-Requested-With: XMLHttpRequest
8 Sec-Ch-Ua-Mobile: ?
9 Authorization: Bearer
eyJhbGciOiJSUzInIiInIisInIdCI6IjFlbmQtSER4eEgtZkZjeXl
Xby1DTmpnOVVFcyJ9.eyJpc3MiOiJlcjm46b2lkOjEuM140IiwiY
XVkijoiaHR0cHM6Ly5b2NhbGhvC3Q6D0A4MS92aWV3ZXiiLCJz
dWIiOjybj290IiwiU3ViamVjdE1Eijoicm9vdCisIkNbhsQuaWN
hbFvZ2XJJZCIEInVp2Dlyb290LGRjPWRvbWPpbixkYz1sb2Nhbc
ISiIN1Ymp1Y3RFcmdbmleYXRpb24iOlsirXkbhXBsZSBPcmdb
m16YXRpb24iXSwicm5sZXMiOlsQ2xpblmjYWxBZGlpbmlzdHjh
dG9ycyIsIiIN5c3R1bUFkbWuaXN0cmFOb3JzI10sIiIN1Ymp1Y3R
Sb2x1IjpbeYjb2R1Ijo1Q2xpblmjYWxBZGlpbmlzdHjhG9ycy
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Type: application/json; charset=UTF-8
5 Date: Mon, 30 Jan 2023 06:10:10 GMT
6 Expires: 0
7 Forcare.com-Logcontext: 79a0f001e495/viewer-281391
8 Vary: accept-encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Xss-Protection: 1; mode=block
12 Content-Length: 8127
13 Connection: close
14
15 {
  "result": [
    {
      "warnings": [
        {
          "document": {
            "id": "fc78770-e9c-48e-7e1237d9f59",
            "loginalid": "c137870-ecb-4be-bead-74e1217d8f59",
            "name": "John Doe",
            "objectType": "STABLE_DOCUMENT",
            "home": "+1.2.3.",
            "logonTime": "19900311",
            "hash": "1a127f1900010c027a5bc0d17a41b3d57b526",
            "languageCode": "en-US",
            "referenceTime": "19900311T12:37",
            "serviceStartTime": "19900311",
            "serviceStopTime": "19900311",
            "source": "Patient ID: 134024500***41.3.6.1.4.1.21367.2005.3.74190",
            "sourcePatientInfo": [
              {"id": "fc78770-e9c-48e-7e1237d9f59", "version": "1.3.6.1.4.1.21367.2005.3.74190", "pid": "51Atweig9Geric", "pid7": "19671111", "pid8": "01-R"}, {"id": "fc78770-e9c-48e-7e1237d9f59", "version": "1.3.6.1.4.1.21367.2005.3.74190", "pid": "51Atweig9Geric", "pid7": "19671111", "pid8": "01-R"}]
        }
      ]
    }
  ]
}
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.8 Webapp: HTTP Strict Transport Security (HSTS) Not Implemented

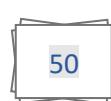
Vulnerability Title	HTTP Strict Transport Security (HSTS) Not Implemented
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.8 CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L
Description	<p><b>Vulnerability Description:</b> The server does not implement the "HTTP Strict-Transport Security" (HSTS) web security policy mechanism. When HSTS is enabled, the web application sends a special response header, "Strict-Transport-Security" to the client with a duration of time specified. Once a supported browser receives this header, that browser can only make requests to the application over HTTPS for the duration of time specified in the header. Any links to resources over HTTP will be rewritten to HTTPS before the request is made.</p> <p><b>Retest (23-Oct-2023):</b> Issue exists in Retest</p> <p><b>Exploitability Rational:</b> Applications that do not utilize the "HTTP Strict-Transport Security" policy are more susceptible to man-in-the-middle attacks via SSL stripping, which occurs when an attacker transparently downgrades a victim's communication with the server from HTTPS to HTTP. Once this is accomplished, the attacker will gain the ability to view and potentially modify the victim's traffic, exposing sensitive information and gaining access to unauthorized functionality.</p> <p>Attacker can gain sensitive information and access for the unauthorized functionality.</p> <p><b>Impact Rational:</b> Attacker can gain sensitive information and access for the unauthorized functionality.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a></p> <p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload</a></p>
<b>Recommendation</b>	<p>The application server should send the "Strict-Transport-Security" HTTP header in each response indicating that future requests to the domain use only HTTPS. The following is a basic example of the HSTS HTTP header, setting a max-age of one year:</p> <p>Strict-Transport-Security: max-age=31536000</p> <p>Subdomains should also be configured in this manner, by including the "includeSubDomains" flag:</p> <p>Strict-Transport-Security: max-age=31536000; includeSubDomains;</p>
<b>Status</b>	<b>OPEN</b>

**Steps to Reproduce:****Retest (23-Oct-2023)****Supported Evidences:**

Request	Response
<pre>Pretty Raw Hex 1 GET /admin/admin/overview.html HTTP/2 2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=EC54/E049ACAD5E3AC6503B8A4FU2BD4 4 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36 root@49bukytihvd65ozgw5uthjrl17c24gt.oastify.com 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/ webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: http://ujhkuo38r7nlgvypqmfk37thb8h2cw0l.oastify.com/ref 9 Dnt: 1 0 Upgrade-Insecure-Requests: 1 1 Sec-Fetch-Dest: document 2 Sec-Fetch-Mode: navigate 3 Sec-Fetch-Site: same-origin 4 Sec-Fetch-User: ?1 5 Sec-Gpc: 1 6 Te: trailers 7 Cache-Control: no-transform 8 9</pre>	<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Cache-Control: post-check=0, pre-check=0 4 Content-Type: text/html; charset=UTF-8 5 Date: Mon, 23 Oct 2023 05:12:49 GMT 6 Expires: 0 7 Force.com-LogonContext: f90178012241/admin-104800 8 X-Content-Type-Options: nosniff 9 X-FRAME-Options: SAMEORIGIN 10 X-UA-Compatible: IE=Edge 11 X-Xss-Protection: 1; mode=block 12 Content-Length: 1991 13 14 &lt;!DOCTYPE html&gt; 15 &lt;!-- 16 (C) Koninklijke Philips N.V., 2006. All rights reserved. 17 --&gt; 18 &lt;html&gt; 19   &lt;head&gt; 20     &lt;link rel="shortcut icon" href="/admin/2302-22/img/favicon.ico" type="image/x-icon" /&gt; 21     &lt;link rel="stylesheet" href="/admin/2302-22/css/admin.css" type="text/css" /&gt; 22     &lt;link rel="stylesheet" href="/admin/2302-22/js/codemirror/lib/codemirror.css" type="text/css" /&gt; 23     &lt;link rel="stylesheet" href="/admin/2302-22/css/custom.css" type="text/css" /&gt; 24   &lt;/head&gt; 25</pre>

**Retest (06-Jun-2023):**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Intercept HTTP history WebSockets history ⚙️ Proxy settings

Filter Not matching expression Strict-Transport-Security

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time
7620	https://3.71.200.223	GET	/admin/services/organization/list.json			200	3647	JSON	json			✓	3.71.200.223		164104 6 Jun
7628	https://3.71.200.223	GET	/admin/services/user/filter?userNameFilter=			200	22532	JSON	json			✓	3.71.200.223		164104 6 Jun
7607	https://3.71.200.223	GET	/admin/2301-26/img/button/button.svg			200	2972	XML	svg			✓	3.71.200.223		164104 6 Jun
7626	https://3.71.200.223	GET	/admin/services/admin/components/index/status/retrieve.json?format=true			✓	200	1255458	JSON	json		✓	3.71.200.223		164104 6 Jun
7625	https://3.71.200.223	GET	/admin/services/admin/components/connect/status/retrieve.json?format=true			✓	200	114497	JSON	json		✓	3.71.200.223		164104 6 Jun
7624	https://3.71.200.223	GET	/admin/services/admin/components/cca/status/retrieve.json?format=true			✓	200	2384519	JSON	json		✓	3.71.200.223		164104 6 Jun
7623	https://3.71.200.223	GET	/admin/services/admin/components/audit/status/retrieve.json?format=true			✓	200	1337926	JSON	json		✓	3.71.200.223		164104 6 Jun
7622	https://3.71.200.223	GET	/admin/2301-26/img/toolbar/small-tuning.svg			200	1391	XML	svg			✓	3.71.200.223		164104 6 Jun

Request

Pretty Raw Hex

```
1 GET /admin/services/users/list.json?userNameFilter= HTTP/1.1
2 Host: 3.71.200.223
3 Cookie: JSESSIONID=177A11A3ADEF84B10C6109C71EDC6D0
4 Sec-Ch-Ua: "Chromium";v="105", "Not A Brand";v="99"
5 Content-Type: application/x-www-form-urlencoded
6 X-Requested-With: XMLHttpRequest
7 Sec-Ch-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/114.0.5735.91 Safari/537.36
10 Sec-Ch-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
11 Accept: */*
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.71.200.223/admin/admin/overview.html
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Length: 1529
5 Content-Type: application/json; charset=UTF-8
6 Date: Tue, 06 Jun 2023 11:11:00 GMT
7 Expires: 0
8 Forcare.com-Logcontext: f90178012241/admin-10757
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Kss-Protection: 1; mode=block
12 Connection: close
13 Content-Length: 2214
14 {
  "result": {
    "complete": true,
    "persons": [
      {
        "dn": "uid=000012310,uid=000000381,ou=practices,ou=users,dc=forcare,dc=local",
        "uid": "00001230",
        "useEmail": "true",
        "mail": "test@forcare.com",
        "givenName": "Otto",
        "objectClass": [
          "top",
          "inetOrgPerson",
          "person",
          "organizationalPerson",
          "overseerPerson"
        ],
        "user": "test-00001230",
        "emp": "Otto test-00001230",
        "rnr": "1000000 Zorginstelling 01",
        "role": [
          {
            "department": ""
          }
        ],
        "dn": "uid=000012352,uid=000000381,ou=practices,ou=users,dc=forcare,dc=local",
        "useEmail": "true"
      }
    ]
  }
}
```

Inspector

- Request attributes
- Request query parameters
- Request cookies
- Request headers
- Response headers

## Old:

2551 https://ec2-3-70-166-239.eu.c... GET /admin/services/admin/queue/retrieve.json 200 216208 JSON json

2548 https://ec2-3-70-166-239.eu.c... GET /admin/services/admin/components/list.json 200 1924 JSON json

Request

Pretty Raw Hex

```
1 GET /admin/services/admin/components/list.json
HTTP/1.1
2 Host:
ec2-3-70-166-239.eu-central-1.compute.amazonaws.com
3 Cookie: JSESSIONID=DEA7AD49BADDE1A7B8B177E13EB4539
4 Sec-Ch-Ua: "Chromium";v="105", "Not A Brand";v="99"
5 Content-Type: application/x-www-form-urlencoded
6 X-Requested-With: XMLHttpRequest
7 Sec-Ch-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/114.0.5735.91 Safari/537.36
10 Sec-Ch-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
11 Accept: */*
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.71.200.223/admin/admin/overview.html
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Length: 1529
5 Content-Type: application/json; charset=UTF-8
6 Date: Mon, 30 Jan 2023 06:47:30 GMT
7 Expires: 0
8 Forcare.com-Logcontext: f90178012241/admin-573864
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Kss-Protection: 1; mode=block
12 Connection: close
13
14 {
  "components": [
    {
      "id": "admin",
      "displayName": "forAdmin",
      "baseUrl": "https://localhost:8081/admin",
      "useEmail": "true"
    }
  ]
}
```

Inspector

- Request Attributes
- Request Cookies
- Request Headers
- Response Headers

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.9 Webapp: No Account Lockout Policy

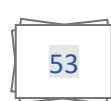
Vulnerability Title	No Account Lockout Policy
Vulnerability Category	A2 - Broken Authentication
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
Description	<p><b>Vulnerability Description:</b> The application does not maintain or enforce an account lockout policy. A lockout policy refers to the mechanism that temporarily suspends a user's account after a certain number of unsuccessful authentication attempts have been made.</p> <p><b>Retest (23-Oct-2023):</b> Issue exists in Retest.</p> <p><b>Exploitability rational:</b> Applications with no lockout policy are vulnerable to brute force password guessing attacks, in which the attacker performs login attempts using a known username and a list of potential passwords until a successful combination is found. Once a successful combination is discovered, the attacker is granted full access to the compromised account and can impersonate the victim without detection.</p> <p><b>Impact rational:</b> Without a strong lockout mechanism, the application can be susceptible to brute force attacks.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload</a>
Recommendation	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Status

OPEN

**Steps to Reproduce:****Retest (23-Oct-2023):****Supported Evidences:****HTTP Request:**

Request	Payload	Status code	Error	Timeout	Length	Comment
39	{base};echo 111111	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
38	`id`	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
37	{base}   ping -i 30 127.0.0.1 ...	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
36	{base))))))))))	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
35	..\..\..\..\..\..\..\..\boot.ini	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
34	../../../../../../../../etc/pass...	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
33	./{base}	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
32	./{base}	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
31	/{base}	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
30	vectact"~`	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
Request	Response					
Pretty	Raw	Hex				
1 POST /admin/services/user/login.json HTTP/2						
2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com						
3 Cookie: JSESSIONID=92FC0E768A86D72C2764E880DA1C1AC						
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0						
5 Accept: */*						
6 Accept-Language: en-US,en;q=0.5						
7 Accept-Encoding: gzip, deflate						
8 Content-Type: application/x-www-form-urlencoded						
9 X-Requested-With: XMLHttpRequest						
10 Content-Length: 45						
11 Origin: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com						
12 Dnt: 1						
13 Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/login.html						
14 Sec-Fetch-Dest: empty						
15 Sec-Fetch-Mode: cors						
16 Sec-Fetch-Site: same-origin						
17 Sec-Gpc: 1						
18 Te: trailers						
19 Connection: keep-alive						
20	j_username=root&j_password={base};echo 111111					
21						

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## HTTP Response:

Request	Payload	Status code	Error	Timeout	Length	Comment
39	{base};echo 111111	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
38	`id`	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
37	{base}   ping -i 30 127.0.0.1 ...	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
36	(base))))))))	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
35	..\..\..\..\..\..\..\..\boot.ini	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
34	../../../../etc/pass...	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
33	./{base}	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
32	/{base}	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
31	/{base}	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
30	vectact"\>\r	401	<input type="checkbox"/>	<input type="checkbox"/>	496	
Request	Response					
Pretty	Raw	Hex	Render			
1	HTTP/2 401 Unauthorized					
2	Cache-Control: no-store, no-cache, must-revalidate					
3	Cache-Control: post-check=0, pre-check=0					
4	Content-Type: text/plain					
5	Date: Mon, 23 Oct 2023 18:27:19 GMT					
6	Expires: 0					
7	Forcare.com-Logcontext: f90178012241/admin-112595					
8	Set-Cookie: JSESSIONID=64A7DA205A62DB4359F4065FA04E9930; Path=/admin; Secure; HttpOnly; SameSite=Lax					
9	X-Content-Type-Options: nosniff					
10	X-Frame-Options: SAMEORIGIN					
11	X-Xss-Protection: 1; mode=block					
12	Content-Length: 32					
13						
14	page.login.action.badCredentials					

Retest (06-Jun-2023):

Steps are same as before.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



100	matrix	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
101	minecraft	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
102	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1600	
<b>Request Response</b>						
<b>Pretty Raw Hex</b>						
<pre> 1 POST /viewer/services/user/login.json HTTP/1.1 2 Host: 3.71.200.223 3 Cookie: JSESSIONID=8C58741349EB362E359300C300D51FF 4 Content-Length: 31 5 Sec-Ch-Ua: 6 Content-Type: application/x-www-form-urlencoded 7 X-Requested-With: XMLHttpRequest 8 Sec-Ch-Ua-Mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.91 Safari/537.36 10 Sec-Ch-Ua-Platform: "" 11 Accept: /* 12 Origin: https://3.71.200.223 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://3.71.200.223/viewer/patient/query.html 17 Accept-Encoding: gzip, deflate 18 Accept-Language: en-US,en;q=0.9 19 Connection: close 20 21 j_username=root&amp;j_password=[REDACTED] </pre>						

### Old POC:

- Login with username and password multiple times then you will be able to see that the account does not get locked out.

Request ▾	Payload	Status	Error	Timeout	Length	Comment
59	w	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
60	x	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
61	y	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
62	z	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
63	root	200	<input type="checkbox"/>	<input type="checkbox"/>	1600	
<b>Request Response</b>						
<b>Pretty Raw Hex</b>						
<pre> 1 POST /admin/services/user/login.json HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=582E698AB59CF9F33E7D2610D97C6192 4 Content-Length: 31 5 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99" 6 Content-Type: application/x-www-form-urlencoded 7 X-Requested-With: XMLHttpRequest 8 Sec-Ch-Ua-Mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 10 Sec-Ch-Ua-Platform: "Windows" 11 Accept: /* 12 Origin: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/login.html 17 Accept-Encoding: gzip, deflate 18 Accept-Language: en-US,en;q=0.9 19 Connection: close 20 21 j_username=root&amp;j_password=[REDACTED] </pre>						

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.10 Webapp: Reflected Cross-Site Scripting (XSS)

Vulnerability Category	Reflected Cross-Site Scripting (XSS)
Vulnerability Category	A3- Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> A Reflected Cross-Site Scripting (XSS) vulnerability occurs when a web application sends strings that are provided by an attacker to a victim's browser in such a way that the browser executes part of the string as code. The string contains malicious data and is passed to the application through a parameter that an attacker can control (For example, a URL parameter or an HTML form field). The application immediately inserts it into its response. This results in the victim's browser executing the attacker's code within a legitimate user's session. Attackers typically exploit reflected XSS vulnerabilities by sending users malicious links containing JavaScript code (For example, via e-mail) or by posting malicious code to other sites that the vulnerable application's users may visit.</p> <p><b>Retest (23-Oct-2023):</b> Issue fixed in retest.</p> <p><b>Exploitability rational:</b> Reflected Cross-Site Scripting vulnerabilities give the attacker control of the user's browser. The attack can alter page content with malicious HTML or JavaScript code. The attacker can arbitrarily alter page content displayed to the victim and can execute application functions using the victim's application identity if the victim is authenticated to the application. An often cited example use of a Reflected Cross-Site is where the attacker send themselves to the victim's session identifier. With this session identifier, the attacker can then perform application functions using that user's identity for the duration of that session.</p> <p><b>Impact rational:</b> Attackers can steal cookies and change the temp look and feel using reflected cross site scripting.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



<b>Affected Systems/IP Address/URL</b>	<p><a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/document/view:medicalDocuments!patientId=7482736282%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO&amp;documentUniqueIds=079bd462-ddcb-4800-9edf-4295e3df6d54">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/document/view:medicalDocuments!patientId=7482736282%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO&amp;documentUniqueIds=079bd462-ddcb-4800-9edf-4295e3df6d54</a></p>
<b>Recommendation</b>	<p>Reflected Cross-Site Scripting (XSS) is prevented by encoding data before inserting it into the generated web page. Each character of the data is encoded and the result string is then inserted onto the generated web page. This technique of encoding values before inserting them on the web page is called "Output Encoding". Output encoding libraries exist for most popular programming languages and frameworks.</p> <p>A web page has seven different output contexts and each output context requires a different encoding scheme. Encode the data using the proper scheme. The seven different encoding schemes are:</p> <ul style="list-style-type: none"> <li>• HTML Text Element</li> <li>• HTML Attribute</li> <li>• URL Parameter</li> <li>• JavaScript Literal</li> <li>• HTML Comment</li> <li>• HTTP Header</li> <li>• CSS Property</li> </ul> <p>For example, the characters: &lt;, &gt;, ", ' are encoded as &amp;#60;, &amp;#62;, &amp;#34;, &amp;#39; for when those characters are inserted into an HTML Text Element. When those characters are inserted as a URL Parameter, the same characters are encoded as %3C, %3E, %22, %27.</p> <p>Libraries for implementing the encoding schemes exist for most popular programming languages.</p> <ul style="list-style-type: none"> <li>• OWASP Java Encoder: Java only</li> <li>• Microsoft Web Protection Library: .NET languages</li> <li>• Ruby – escapeHTML() - only supports HTML Text Encoding</li> <li>• Jencoder in JQuery: for preventing DOM-based XSS</li> </ul> <p>Green field projects can consider the use of other technologies:</p> <ul style="list-style-type: none"> <li>• Google Capabilities based JavaScript CAJA</li> </ul>



	<ul style="list-style-type: none"> <li>OWASP JXT – automatically encodes string data with the proper encoding.</li> </ul> <p>Input validation is often recommended as a way to mitigate reflected cross-site scripting. It is insufficient, however, because input validation is used to prevent cross-site scripting only when the data has a strict syntactic format, such as numeric values and dates. Any application inputs which must accept arbitrary data would remain vulnerable.</p>
Status	CLOSED

#### Steps to Reproduce:

**Retest (23-Oct-2023):**

**Supporting Evidences:**

#### Retest (06-Jun-2023):

Steps are same as mentioned in 'Retest Status( as on 30 Jan 2023)'.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The screenshot shows a web browser window for the HealthSuite Interoperability Viewer. The URL is <https://3.71.200.223/viewer/patient/query.html#/0/document/viewMedicalDocuments?patientId=2503104&SE%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO&documentUniqueId=d2a3463e-b491-471e-8758-5d3f3c423c0>. The page displays a patient record for Pet, Peter (ID: 2503104 (HOS), Jan 1, 1922 (01 yr), Male) with address 24 Lily street, SC Flow city. A modal dialog box is overlaid on the page, containing the text "An embedded page at 3.71.200.223 says" followed by "xss" and an "OK" button. The entire dialog is highlighted with a red box.

### Old POC:

Login to Viewer > Patient search >> select any patient >>> medical documents >>>> Add document >>>> Discharge Note(Ldap lookup) >>>>> fill the form as shown in the below snapshot and then submit, the application server responds with same malicious script without validation or encoding and execute at browser.

The screenshot shows a web browser window for the HealthSuite Interoperability Viewer. The URL is <https://35.176.185.168/viewer/patient/query.html#/0/document/provideMedicalDocuments?patientId=111%5E%5E%5E%262.16.840.1.113883.2.1.4.1%26ISO>. The page displays a patient record for sree<img src="" onerror=alert(1)>, sree<img src="" onerror=alert(2)>. A modal dialog box is overlaid on the page, containing the text "35.176.185.168 says" followed by "101" and an "OK" button. Below the form, a message says "This form is supplied as an example that must be configured prior to using it". The "Role" field contains the XSS payload "sree><img src="" onerror=alert(101)>". A second modal dialog box appears with the message "Something went wrong" and an "OK" button.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Login to Viewer > Patient search >> select any patient >>> medical documents >>> select any xml document >>>> actions >>>>> edit

Parameters: Source Patient ID & Source patient Info

The screenshot shows the Philips XDS interface. At the top, there's a navigation bar with links like 'Home', 'Patient search', 'Patient record', 'Medical documents', 'All exports', 'My Settings', 'Help', and 'About'. Below the navigation, it displays patient information: Address: sree<img src="" onerror=alert(2)>, sree<img src="" onerror=alert(3)>, Date of birth: 23 Feb 1990 (30 yr), Gender: Female, ID: 100120120 (BSN). The main area shows a list of '5 documents' with columns: Creation date, Title, Author, Author's role, Author's institution, and Type. One document in the list has its details highlighted with a red box, including the author's name and role. The 'Edit' button in the toolbar is also highlighted with a red box.

This screenshot shows the 'Edit document' page. It includes fields for Confidentiality, Creation Time, Healthcare Facility Type, Format, Language Code, Person Signing, Practice Setting, Service Start Time, Service Stop Time, and Source Patient Id. The 'Source Patient Id' field is highlighted with a red box and contains the value '100'. A modal dialog box titled 'Something went wrong' is centered on the page, with an 'OK' button at the bottom right.

### Retest Status( as on 30 Jan 2023)

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Issue still persists.

Uploading a pdf which has malicious script.

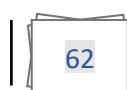
- Upload the file and navigate to Medical Documents section.
- Click the pdf icon for the patient where the document is upload.

- Scroll the launched pdf and you can see the JavaScript getting executed.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.11 Webapp: Weak SSL/TLS Configuration

Vulnerability Title	Weak SSL/TLS Configuration
Vulnerability Category	A2 Cryptographic Failures
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> It is observed that the server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites in the provided server.</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)</p> <p><b>Retest (23-Oct-2023):</b> Issue exists in Retest.</p> <p><b>Exploitability Rational:</b> Some misconfiguration in the server can be used to force the use of a weak cipher - or at worst no encryption - permitting to an attacker to gain access to the supposed secure communication channel. Other misconfiguration can be used for a Denial-of-Service attack.</p> <p><b>Impact Rational:</b> A server-side SSL/TLS endpoint that supports weak ciphers can allow an attacker to read or modify traffic sent in SSL/TLS connections with that endpoint.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com</a>
Recommendation	<p>Update the server-side TLS endpoint's configuration to allow only TLSv1.2 or TLSv1.3 connections with cipher suites that use the following:</p> <ul style="list-style-type: none"> <li>• Ephemeral Diffie-Hellman for key exchange (Optionally, allow RSA for key exchange if necessary for supporting some clients).</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<ul style="list-style-type: none"> <li>Block ciphers in GCM mode. Note: If CBC mode must be allowed for supporting some clients, use only CBC mode cipher suites that use the SHA2 family of hash functions (SHA256, SHA384, SHA512).</li> </ul>
Status	OPEN

### Steps to Reproduce:

Retest (23-Oct-2023):

### Supported Evidences:

```
Testing SSL server ec2-3-71-200-223.eu-central-1.compute.amazonaws.com on port 443 using SNI name ec2-3-71-200-223.eu-central-1.compute.amazonaws.com

SSL/TLS Protocols:
SSLv2    disabled
SSLv3    disabled
TLSv1.0  disabled
TLSv1.1  disabled
TLSv1.2  enabled
TLSv1.3  enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSV1.3 128 bits TLS_AES_128_GCM_SHA256      Curve 25519 DHE 253
Accepted  TLSV1.3 256 bits TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Accepted  TLSV1.3 256 bits TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Preferred TLSV1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSV1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSV1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305  Curve 25519 DHE 253
Accepted  TLSV1.2 128 bits ECDHE-RSA-AES128-SHA         Curve 25519 DHE 253
Accepted  TLSV1.2 256 bits ECDHE-RSA-AES256-SHA         Curve 25519 DHE 253
Accepted  TLSV1.2 128 bits AES128-GCM-SHA256            Curve 25519 DHE 253
Accepted  TLSV1.2 256 bits AES256-GCM-SHA384           Curve 25519 DHE 253
Accepted  TLSV1.2 128 bits AES128-SHA                   Curve 25519 DHE 253
Accepted  TLSV1.2 256 bits AES256-SHA                   Curve 25519 DHE 253
Accepted  TLSV1.2 112 bits ECDHE-RSA-DES-CBC3-SHA       Curve 25519 DHE 253
Accepted  TLSV1.2 112 bits DES-CBC3-SHA                  Curve 25519 DHE 253
```

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS • Host ec2-3-71-200-223.e

```
nmap -sS -p 443 -Pn --script ssl* ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-21 18:03 India Standard Time
Nmap ERROR [0.0410s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for ec2-3-71-200-223.eu-central-1.compute.amazonaws.com (3.71.200.223)
Host is up (0.15s latency).

PORT      STATE SERVICE
443/tcp    open  https
| ssl-cert: Subject: commonName=test/organizationName=Philips International BV/stateOrProvinceName=North Holland/countryName=NL
| Issuer: commonName=Root CA/organizationName=Philips International BV/stateOrProvinceName=North Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-01-29T11:30:29
| Not valid after:  2025-01-27T11:30:29
| MD5:  5a322fc2ad52af511e4f54753ec088d4
|_SHA-1: 6cf7ccc196142c5dcfd005a435b8363c0b33d4e
|_ssl-date: TLS randomness does not represent time
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS RSA WITH AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|     cipher preference: server
|     least strength: C
|_  Nmap done: 1 IP address (1 host up) scanned in 17.48 seconds
```

### Retest (06-Jun-2023):

Steps are same as before.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



```
xds_443_ssl_enum X
1 # Nmap 7.93 scan initiated Mon May 29 14:13:19 2023 as: nmap -p 443 --script=ssl* -oN nmap/xds_443_ssl_enum -v -d 18.196.27.233
2 ----- Timing report -----
3 hostgroups: min 1, max 100000
4 rtt-timeouts: init 1000, min 100, max 10000
5 max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
6 parallelism: min 0, max 0
7 max-retries: 10, host-timeout: 0
8 min-rate: 0, max-rate: 0
9 -----
10 Nmap scan report for ec2-18-196-27-233.eu-central-1.compute.amazonaws.com (18.196.27.233)
11 Host is up, received syn-ack (0.165 latency).
12 Scanned at 2023-05-29 14:13:20 IST for 12s
13
14 PORT      STATE SERVICE REASON
15 443/tcp    open  https   syn-ack
16 | ssl-enum-ciphers:
17 |   TLSv1.2:
18 |     ciphers:
19 |       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
20 |       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
21 |       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
22 |       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
23 |       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
24 |       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa_2048) - A
25 |       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa_2048) - A
26 |       TLS_RSA_WITH_AES_128_CBC_SHA (rsa_2048) - A
27 |       TLS_RSA_WITH_AES_256_CBC_SHA (rsa_2048) - A
28 |       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
29 |       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa_2048) - C
30 | compressors:
31 |   NULL
32 | cipher preference: server
33 | warnings:
34 |   64-bit block cipher 3DES vulnerable to SWEET32 attack
```

### Old POC:

Use Nmap to enumerate the ciphers used by the application endpoints.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-23 18:30 India Standard Time  
Nmap scan report for ec2-3-70-166-239.eu-central-1.compute.amazonaws.com (3.70.166.239)  
Host is up (0.14s latency).

```
PORt      STATE SERVICE
443/tcp   open  https
| ssl-enum-ciphers:
|_ TLSv1.2:
|   ciphers:
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|     TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa_2048) - A
|     TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa_2048) - A
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa_2048) - A
|     TLS_RSA_WITH_AES_256_CBC_SHA (rsa_2048) - A
|     TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa_2048) - C
| compressors:
|   NULL
| cipher preference: server
| warnings:
|   64-bit block cipher 3DES vulnerable to SWEET32 attack
TLSv1.3:
| ciphers:
|   TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|   TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|   TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
| cipher preference: server
|_ least strength: C

Nmap done: 1 IP address (1 host up) scanned in 12.22 seconds
```



## 8.12 Webapp: Missing Security Header

Vulnerability Title	Missing Security Header
Vulnerability Category	A5 Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.9 CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L
Description	<p><b>Vulnerability Description:</b> During security assessment, we found that either the security headers are not configured properly, or security headers are missing in response. Security headers in the response can be used to increase the security of the application.</p> <p>The missing security headers are:</p> <ul style="list-style-type: none"> <li>Content-Security-Policy</li> </ul> <p><b>Exploitability Rational:</b> Exploitability of these depends differently based on the missing headers. Like Cache-Control headers require physical access to the system. But others require user interaction to exploit this vulnerability.</p> <p><b>Impact Rational:</b> These headers provide the additional security at client side. Missing these headers may lead to sensitive information disclosure like account take over etc.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit</a> <a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload/?assigningAuthority=1.3.6.1.4.1.21367.2005.3.7#/start">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload/?assigningAuthority=1.3.6.1.4.1.21367.2005.3.7#/start</a>
Recommendation	It is recommended to configure all the security headers in the response to improve your application's security.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Status	OPEN
--------	------

### Steps to Reproduce:

### Supportive Evidences:

Screenshot of a browser developer tools Network tab showing a request to `/admin/application/info/retrieve.json` and its response.

**Request Headers:**

```

GET /admin/application/info/retrieve.json HTTP/2
Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
Cookie: JSESSIONID=9ADDEB5439F5C5D754790D700244426
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5750.110 Safari/537.36
Sec-Ch-Platform: ""
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/admin/overview.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

**Response Headers:**

```

HTTP/2 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Content-Type: application/json; charset=UTF-8
Date: Mon, 23 Oct 2023 11:15:05 GMT
Expires: -
Forage.com-LogonContext: f9017801c241/admin-108665
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 663

```

**Response Body:**

```
{
  "applicationInfo": {
    "connectPath": "/admin",
    "producer": "forkAmine",
    "isCRegistered": false,
    "license": "",
    "serial": "10053"
}
```

CSP not set

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.13 Webapp: Server Banner Disclosure

Vulnerability Title	Server Banner Disclosure
Vulnerability Category	A5 Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment, it was found that the application discloses the application server details including the version in the HTTP response. Targeted attacks can be launched against the server based on the exploits it is having.</p> <p><b>Exploitability Rational:</b> Web server fingerprinting is a critical task for the penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing and those are available on internet.</p> <p><b>Impact Rational:</b> Targeted attacks can be launched against the server based on the exploits it is having.</p>
Affected Systems/IP Address/URL	<a href="https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin</a>
Recommendation	It is recommended to use custom banner for server by hiding all sensitive information from banner.
Status	<b>OPEN</b>

**Steps to Reproduce:**

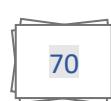
**Supported Evidences:**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Send Cancel < > Target: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers
<pre>1 GET /admin/services/admin/components/workflow/status/retrieve.json?format=true HTTP/1.1 2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=ECCE0146ED73C30515DBD045A5C90E9C 4 Sec-Ch-Ua:  5 Content-Type: application/x-www-form-urlencoded 6 X-Requested-With: XMLHttpRequest 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5750.110 Safari/537.36 9 Sec-Ch-Ua-Platform:  10 Accept: */* 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/admin/overview.html 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 18</pre>	<pre>1 HTTP/1.1 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Pragma: no-cache 4 Content-Type: application/json;charset=UTF-8 5 Date: Mon, 23 Oct 2023 11:47:16 GMT 6 Expires: 0 7 Server: com-Logcontext: 94ffe7557eaf@workflow-4570 8 Vary: Accept-Encoding 9 X-Content-Type-Options: nosniff 10 X-Frame-Options: SAMEORIGIN 11 X-Xss-Protection: 1; mode=block 12 13 { 14     "status": "STARTED", 15     "licensed": true, 16     "registered": false, 17     "accessControlEnabled": false, 18     "logLevel": "INFO", 19     "revision": "13", 20     "externalVersion": "0003-0", 21     "serverInfo": "Apache Tomcat/9.0.71", 22     "hasVisibleFiles": true, 23     "wacu2zIpEncryptionSupport": true, 24     "advices": [ 25         { 26             "canAutoFix": true, 27             "canTune": false, 28             "description": "This advice forces server tuning.AuditQueueTuningAdvisor", 29             "longDescription": "Auditing using TCD with multiple queue-workers will not have any effect", 30             "multipleAdvisors": "Multiple audit queue workers will always use the same Audit TCP sender instance therefore have no performance improvement.", 31             "resolutionDescription": "Enabling AuditQueueTuningAdvisor to utilize the multiple number of workers in the audit queue." 32         }, 33         { 34             "canAutoFix": false, 35             "canTune": false 36         } 37     ] 38 }</pre>	Activate Windows

### Apache Tomcat/9.0.71

Send Cancel < > Target: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers
<pre>1 DELETE /admin/services/admin/components/workflow/status/retrieve.json?format=true HTTP/1.1 2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=ECCE0146ED73C30515DBD045A5C90E9C 4 Sec-Ch-Ua:  5 Content-Type: application/x-www-form-urlencoded 6 X-Requested-With: XMLHttpRequest 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5750.110 Safari/537.36 9 Sec-Ch-Ua-Platform:  10 Accept: */* 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/admin/overview.html 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 18</pre>	<pre>HTTP Status 405 - Method Not Allowed &lt;/html&gt; &lt;hr class="line" /&gt; &lt;p&gt;&lt;b&gt;Type&lt;/b&gt;&lt;/p&gt; &lt;p&gt;&lt;b&gt;Status Report&lt;/b&gt;&lt;/p&gt; &lt;p&gt;&lt;b&gt;Message&lt;/b&gt;&lt;/p&gt; &lt;p&gt;&lt;b&gt;Description&lt;/b&gt;&lt;/p&gt; &lt;p&gt;The method received in the request-line is known by the origin server but not supported by the target resource.&lt;/p&gt; &lt;hr class="line" /&gt; &lt;p&gt;Apache Tomcat/9.0.71&lt;/p&gt; &lt;/body&gt; &lt;/html&gt;</pre>	Activate Windows

### Apache Tomcat/9.0.71

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





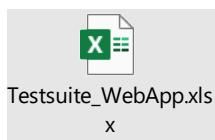
## 9. Tools Used

Scope	Tools Used
Web Application Security	Burpsuite pro, nmap

## 10. Automated Tool Report

NA

## 11. Manual Test Reports and Test Case Execution



PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.